Lecture 24: Skew-fields, I.

1) Main results.

2) Tensor products of algebras.

Ref: [V], Sec 11.6.

1) Main results.

Our goal in the remaining two lectures is to apply the results about (semi) simple algebras to understand the structure of skew-fields. Let $\mathbb{F}$ be a field and S be a finite dimensional $\mathbb{F}$-algebra that is a skew-field.

1.1) Commutative subalgebras.

To state our main structural result we need a few observations about commutative subalgebras of S.

Lemma: Every commutative $\mathbb{F}$-subalgebra $C \subset S$ is a field.

Proof: We need to show $x \in C \setminus \{0\} \Rightarrow x^{-1} \in C$. Since $\dim_{\mathbb{F}} S < \infty$,

$\exists\, n>0$ & $a_0, \dots a_{n-1} \in \mathbb{F} \mid x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$. We can assume $a_0 \neq 0$, otherwise divide by x. Then $x^{-1} = -\frac{1}{a_0}(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1) \in C$ $\square$

Corollary: Let A be a simple $\mathbb{F}$-algebra. Then $Z(A)$ is a field.

Proof:

By the classification of simple algebras (Sec 2.3 of Lec 22), $A \simeq Mat_n(S)$ for S as above. By Exercise in Sec 2 of Lec 23, $Z(A) \simeq Z(S)$. By Lemma, $Z(S)$ is a field. $\square$

Definition: We say that A (as in Corollary) is central if $Z(A) = \mathbb{F}$.

We note that A is always central if viewed as algebra over $Z(A)$ (which is a finite field extension of $\mathbb{F}$). This allows one to only consider central simple algebras.

Exercise: If S is a skew-field, then every maximal subfield contains $Z(S)$.

1.2) Statement

We are interested in the structure of maximal (w.r.t. $\subseteq$) subfields (equivalently, commutative subalgebras) of S.

Theorem: Suppose $\operatorname{char} \mathbb{F} = 0$. Suppose S is central. Then the following hold:

1) $\forall$ maximal subfields $K_1, K_2 \subset S$, have $\dim_{\mathbb{F}} K_1 = \dim_{\mathbb{F}} K_2$.

2) if the dimension in 1) is n, then $\dim_{\mathbb{F}} S = n^2$.

3) Let K_1, K_2 be maximal subfields and $\tau: K_1 \xrightarrow{\sim} K_2$ be an $\mathbb{F}$-linear isomorphism. Then $\exists\, s \in S \setminus \{0\} \mid \tau(x) = sxs^{-1}\ \forall x \in K_1$.

Rem: The same is true if $\operatorname{char} \mathbb{F} = p$ assuming $\mathbb{F}$ is perfect (every element has pth root). In general, one has a complete analog of this theorem, where one considers maximal subfields of S that are separable over $\mathbb{F}$: one can show that there is a maximal subfield, which is separable.

1.3) Application: Frobenius theorem

We will prove the theorem later, and now we will explain it's famous application.

Corollary (Frobenius): Every skew-field S, which is a finite dimensional $\mathbb{R}$-algebra is $\mathbb{R}, \mathbb{C}$, or $\mathbb{H}$.

Proof: $\mathbb{C}$ is the only nontrivial finite field extension of $\mathbb{R}$. Thx to 1)&2) of Thm, we only need to show that if $Z(S)=\mathbb{R}$ & dimension of the maximal subfields in S is 2 (in which case all of them are isomorphic to $\mathbb{C}$), then $S \simeq \mathbb{H}$.

Step 1: Pick a copy of $\mathbb{C}$ in S and view S as a $\mathbb{C}$-vector space via multiplication on the left. By 2) of Thm, $\dim_{\mathbb{R}} S=4$, so $\dim_{\mathbb{C}} S=2$. Let $i:=\sqrt{-1}\in\mathbb{C}$ viewed as an element of S. Our goal is to find $j\in S$ w. $j^2 \overset{?}{=} -1$, $ji=-ij$, then we are done.

Step 2: Apply 3) of Thm to $\tau(z)=\bar{z}: \mathbb{C} \xrightarrow{\sim} \mathbb{C}$. We get

$s \in S$ w $szs^{-1} = \bar{z}$ $\forall z \in \mathbb{C} \Leftrightarrow sis^{-1} = -i$. Note that:

(i) $s \notin \mathbb{C}$ b/c $\mathbb{C}$ is commutative. So $1, s$ form a basis in the $\mathbb{C}$-vector space S.

(ii) $s^2 \in \mathbb{R}$, equivalently, s is central. This is because s^2 commutes w. s & w. $\mathbb{C}$: $s^2 z s^{-2} = s(szs^{-1})s^{-1} = \bar{\bar{z}} = z$. By (i), $\mathbb{C}$ & s generate S as a ring, so s^2 is central.

Step 3: Let $s^2 = a (\in \mathbb{R} \setminus \{0\})$. We have $a < 0$ (otherwise $(s - \sqrt{a})(s + \sqrt{a}) = 0$ (b/c $\sqrt{a} \in \mathbb{R}$ commutes w. s) so $s = \pm\sqrt{a} \in \mathbb{R}$ leading to a contradiction. Now set $j := s/\sqrt{-a}$ getting $jij^{-1} = -i$ $\Leftrightarrow ji = -ij$ & $j^2 = -1$. This finishes the proof. $\square$

Side remark:

Using the same techniques one can classify 4-dimensional skew-fields over a field $\mathbb{F}$ of char $\neq 2$. Namely pick $a, b \in \mathbb{F} \setminus \{0\}$. Form the generalized quaternion algebra $\mathbb{H}(a, b)$: it has basis $1, i, j, k$ w. multiplication recovered from $i^2 = a$, $j^2 = b$, $k = ij = -ji$ (in particular, $k^2 = -ab$).

Exercise*: 1) $\mathbb{H}(a,b)$ is a skew-field $\Leftrightarrow$ the equation $x^2-ay^2-bz^2+abu^2=0$ doesn't have nonzero solutions in $\mathbb{F}$. Hint: $(x+yi+zj+uk)(x-yi-zj-uk) = x^2-ay^2-bz^2+abu^2$.

2) Suppose Theorem holds for S of dim 4 (e.g. if char $\mathbb{F}=0$, in fact, the theorem here holds as long as char $\mathbb{F}\neq 2$). Then $S\simeq \mathbb{H}(a,b)$ for some a,b.

3) Give an example when S contains non-isomorphic maximal subfields.

2) Tensor products of algebras.

The main basic ingredient in the proof of the theorem is "base change to the algebraic closure of $\mathbb{F}$": if $\overline{\mathbb{F}}$ denotes the algebraic closure, then we seek to replace $\mathbb{F}$-algebras w. suitable $\overline{\mathbb{F}}$-algebras. Then we use the fact that the classification of simple algebras over $\overline{\mathbb{F}}$ is easier than in the general case: they are just matrix algebras $\mathrm{Mat}_n(\overline{\mathbb{F}})$.

The base change is a special case of a more general construction of taking certain tensor products. The complexification (= passing from $\mathbb{R}$ to $\mathbb{C}$) in HW2 is a special case.

2.1) Construction of tensor product of algebras.

We start w. two $\mathbb{F}$-vector spaces A, B equipped with $\mathbb{F}$-bilinear maps $\mu_A: A\times A \longrightarrow A$, $\mu_B: B\times B \longrightarrow B$. Form the tensor product $A\otimes B$ (over $\mathbb{F}$). We'll need the situation when A or B is infinite dimensional. Still A & B have bases: $a_i\in A$, $i\in I$, $b_j\in B$, $j\in J$, where I, J are some sets. Then the elements $a_i\otimes b_j$ form a basis in $A\otimes B$.

Lemma: i) $\exists!$ bilinear map $\mu_{A\otimes B}: A\otimes B\times A\otimes B \longrightarrow A\otimes B$ w.

(1) $$\mu_{A\otimes B}(a\otimes b, a'\otimes b') = \mu_A(a,a')\otimes \mu_B(b,b')$$

ii) If μ_A, μ_B are associative (resp. commutative, resp. $\exists$ units), then $\mu_{A\otimes B}$ is associative (resp. commutative, resp. $\exists$ unit).

Sketch of proof:

i) Let $\mu_{A\otimes B}$ be the unique bilinear map w.

(2) $$\mu_{A\otimes B}(a_i\otimes b_j, a_\ell\otimes b_k) = \mu_A(a_i,a_\ell)\otimes \mu_B(b_j,b_k) \;\forall\, i,\ell\in I,\, j,k\in J$$

(where $a_i, i\in I$, $b_j, j\in J$ are bases in A & B). To check $\mu_{A\otimes B}$

satisfies (1) is an exercise. On the other hand, (1) $\Rightarrow$ (2) so $\mu_{A\otimes B}$ is unique. This proves i).

2) Let's prove μ_A, μ_B are commutative $\Rightarrow \mu_{A\otimes B}$ is commutative:

$$\mu_{A\otimes B}(x_1, x_2) = \mu_{A\otimes B}(x_2, x_1) \quad \forall x_1, x_2 \in A\otimes B.$$

If $x_i = \alpha_i \otimes \beta_i$, $i = 1, 2$, then

$$\mu_{A\otimes B}(x_1, x_2) = \mu_A(\alpha_1, \alpha_2) \otimes \mu_B(\beta_1, \beta_2) = \mu_A(\alpha_2, \alpha_1) \otimes \mu_B(\beta_2, \beta_1) = \mu_{A\otimes B}(x_2, x_1)$$

In general, $x_i = \sum_j \alpha_i^j \otimes \beta_i^j$, and we reduce to the previous case by bilinearity.

The claims about associativity & unit are proved in a similar fashion (if $1_A \in A$, $1_B \in B$ are units, then so is $1_A \otimes 1_B \in A\otimes B$). $\square$

Thx to the lemma, if A, B are associative algebras, then $A\otimes B$ acquires the natural associative algebra structure (called the tensor product of algebras).

Exercise: 1) For an $\mathbb{F}$-algebra A, $\mathrm{Mat}_n(\mathbb{F}) \otimes A \simeq \mathrm{Mat}_n(A)$.

Hint: $E_{ij} \otimes a \mapsto a E_{ij}$.

2) $\mathrm{Mat}_n(\mathbb{F}) \otimes \mathrm{Mat}_m(\mathbb{F}) \simeq \mathrm{Mat}_{mn}(\mathbb{F})$.

Remarks: 1) Notice that the maps $A \longrightarrow A\otimes B$, $a \mapsto a\otimes 1$, $B \longrightarrow A\otimes B$, $b \mapsto 1\otimes b$ are algebra homomorphisms.

2) If M is an A-module, N is a B-module, then $M\otimes N$ has the unique $A\otimes B$-module structure with

$$(a\otimes b).(m\otimes n) = (am)\otimes(bn).$$

The proof follows that of Lemma and is left as an exercise.

3) The tensor product of algebras is associative ($(A\otimes B)\otimes C \simeq A\otimes(B\otimes C)$), commutative, distributive (w.r.t. $\oplus$) and $\mathbb{F}$ is a unit ($\mathbb{F}\otimes A \simeq A\otimes\mathbb{F} \simeq A$): the natural isomorphisms of Sec 1.4 are those of algebras.

2.2) Base change

We will be interested in the special case, where B is a field $\widetilde{\mathbb{F}}$ containing $\mathbb{F}$ (a.k.a. a field extension). We write:

(i) for an $\mathbb{F}$-vector space V, $V_{\widetilde{\mathbb{F}}} := V \otimes \widetilde{\mathbb{F}}$. This is a module over $\mathbb{F} \otimes_{\mathbb{F}} \widetilde{\mathbb{F}} = \widetilde{\mathbb{F}}$, i.e. a vector space over $\widetilde{\mathbb{F}}$.

(ii) for an $\mathbb{F}$-algebra A, $A_{\widetilde{\mathbb{F}}} := A \otimes \widetilde{\mathbb{F}}$. This is an algebra over $\widetilde{\mathbb{F}}$.

(iii) for an A-module M, $M_{\widetilde{\mathbb{F}}} := M \otimes \widetilde{\mathbb{F}}$. This is a module over $A_{\widetilde{\mathbb{F}}}$.

We say that $V_{\widetilde{\mathbb{F}}}, A_{\widetilde{\mathbb{F}}}, M_{\widetilde{\mathbb{F}}}$ are obtained from V, A, M by base change to $\widetilde{\mathbb{F}}$.

Remark: Here's how one thinks about base change in practice. Suppose that an algebra A is finite dimensional, for simplicity. Choose a basis $a_1, \dots a_n \in A$, and write the multiplication table:

$$a_i a_j := \sum_{k=1}^{n} \alpha_{ij}^k a_k, \quad \alpha_{ij}^k \in \mathbb{F}.$$

Then $A_{\widetilde{\mathbb{F}}}$ has basis $a_i \otimes 1$ (now over $\widetilde{\mathbb{F}}$) & the same multiplication table.